Osnovna šola Vrhovci
Cesta na Bokalce 1
1000 Ljubljana
Št.: 6042-1/2022/40
Datum: 25. 4. 2023

☎ 01 423 03 70
e-naslov: tajnistvo@os-vrhovci.si
spletna stran: www.os-vrhovci.si
TRR: SI56 0126 1603 0665 280
ID za DDV: SI34317627

PRAVILNIK O VARSTVU OSEBNIH PODATKOV OSNOVNE ŠOLE VRHOVCI

Dokument se začne uporabljati od 26. 4. 2023

Ravnateljica

Marjanca Vampelj

MARJANCA VAMPELJ

Digitally signed by MARJANCA VAMPELJ
Date: 2023.04.26 10:38:12 +02'00'

KAZALO

1. PREAMBULA

Ta pravilnik o varstvu osebnih podatkov je sprejet 25. 4. 2023 s strani zakonitega zastopnika upravljavca na podlagi 24., 25. in 32. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju Splošna uredba o varstvu podatkov oz. GDPR).

2. SPLOŠNE DOLOČBE

1. člen

(Uvodna določba)

S tem pravilnikom se določajo tehnični in organizacijski ukrepi za zagotavljanje varstva osebnih podatkov posameznikov, ki jih upravlja oziroma obdeluje upravljavec osebnih podatkov.

Upravljavec OŠ Vrhovci je z doslednim izvajanjem ukrepov zmožen dokazati, da obdelava poteka v skladu z veljavnimi predpisi s področja varstva osebnih podatkov, da je skladen z vsemi načeli obdelave osebnih podatkov iz 5. člena Splošne uredbe o varstvu podatkov vključno tudi da zagotavlja zaupnost, celovitost, razpoložljivost in točnost osebnih podatkov.

2. člen

(Namen in vsebina pravilnika)

Namen pravilnika je opredeliti namen in obseg obdelave osebnih podatkov vključno z razmejitvijo vlog in odgovornostjo upravljavca, obdelovalcev in uporabnikov osebnih podatkov, pravno podlago za obdelavo, določitev tehničnih in organizacijskih ukrepov za zagotovitev varstva pri obdelavi osebnih podatkov, način izvajanja pogodbene obdelave osebnih podatkov, evidence dejavnosti obdelav osebnih podatkov, način uresničevanja pravic posameznikov, politiko ravnanja v primeru varnostnih incidentov ter letni pregled izvajanja aktivnosti varstva podatkov.

3. člen

(Zavezanci)

Določbe tega pravilnika zavezujejo upravljavca, pri njem zaposlene in druge delavce, ki delajo zanj na podlagi pogodb civilnega prava, pooblaščeno osebo za varstvo podatkov in upravljavčeve obdelovalce osebnih podatkov.
Zaposleni in drugi delavci v potrditev seznanitve z določbami tega Pravilnika in zavedanja o pomenu varstva osebnih podatkov podpišejo posebno izjavo **- Izjava za zaposlene in zunanje**, s pogodbenimi obdelovalci sklene upravljavec poleg pogodbe o storitvi tudi pogodbo o obdelavi osebnih podatkov z vsebino iz 28. člena Splošne uredbe o varstvu podatkov **- Pogodba o obdelavi osebnih podatkov**.

4. člen

(Relevantni predpisi in akti)

Poleg Splošne uredbe o varstvu podatkov in Zakona o varstvu osebnih podatkov (ZVOP-2) področje varstva osebnih podatkov urejajo tudi področni predpisi, kot so Zakon o financiranju vzgoje in izobraževanja (ZOFVI), Zakon, ki opredeljuje delovanje posamezne vrste vzgojno izobraževalne ustanove, Zakon o šolski prehrani (ZsolPre-1) in drugi.

5. člen

(Opredelitev pojmov)

V tem pravilniku uporabljeni pojmi imajo naslednji pomen:
1. **upravljavec** je Osnovna šola Vrhovci;
2. **obdelovalec** je fizična ali pravna oseba, ki obdeluje osebne podatke v imenu upravljavca;
3. **pooblaščena oseba za varstvo podatkov** je fizična ali pravna oseba, ki je s strani upravljavca pooblaščena za upravljanje področja varstva podatkov in neposredno poroča zastopniku upravljavca.
Pooblaščeno osebo za varstvo podatkov (t.i. DPO) s sklepom imenuje zastopnik upravljavca in o tem v 30. tih dneh od imenovanja obvesti nadzorni organ.
4. **Interni koordinator za varstvo podatkov** je pri upravljavcu zaposlena oseba, ki je seznanjena z aktivnostmi upravljanja in obdelave osebnih podatkov pri upravljavcu ter praviloma skrbi za implementacijo navodil v primeru, da je upravljavec imenoval zunanjo pooblaščeno osebo za varstvo podatkov;
5. **osebni podatki** so katera koli informacija v zvezi z določenim ali določljivim posameznikom. Določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
6. **posebne vrste osebni podatki** so podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, genetski in biometrični podatki, ki se obdelujejo za namene edinstvene identifikacije posameznika, podatki v zvezi z zdravjem ali podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;
7. **obdelava** je vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

8. **privolitev posameznika** pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero (izjavo ali jasnim pritrdilnim dejanjem) izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj. V primeru, da je posameznik mladoleten, se kot privolitev posameznika po tem pravilniku šteje privolitev njegovega zakonitega zastopnika ali skrbnika;
8. **omejitev obdelave** je označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;

9. **oblikovanje profilov** je vsaka oblika avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika;

10. **psevdonimizacija** je obdelava osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;
11. **kršitev varstva osebnih podatkov** je kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
12. **nadzorni organ** je Informacijski pooblaščenec Republike Slovenije, Dunajska cesta 22, 1000 Ljubljana, Slovenija;
13. **sistemska programska oprema** so programi, ki jih računalnik uporablja za krmiljenje svoje opreme in za komunikacijo z okoljem (operacijski sistem) in druga programska orodja, ki jih dobimo skupaj z operacijskim sistemom in so namenjena vzdrževalcem in uporabnikom računalnika (npr. operacijski sistem Windows 10 ter internetni pregledovalec, ki je del operacijskega sistema);
14. **aplikativna programska oprema** so programi ali z njimi povezane informacijske storitve, s katerimi se izvaja obdelava podatkov (npr. eAsistent, eDelovodnik, eVrtec, eGlasbenaŠola, programska oprema za eHrambo Logitus, finančno računovodski informacijski sistem, ipd..);
15. **zavezanci** po tem pravilniku so vsi zaposleni in drugi pogodbeni sodelavci upravljavca;
16. **obdelovalci** so lahko le tiste osebe, ki sklenejo z upravljavcem pogodbo o obdelavi skladno z 28. členom Splošne uredbe o varstvu podatkov.

3. OBDELAVA OSEBNIH PODATKOV

6. člen

(Obseg, namen in pravna podlaga)

Upravljavec obdeluje le tiste osebne podatke, za katere ima pravno podlago v eni od točk prvega odstavka 6. člena Splošne uredbe o varstvu podatkov oziroma 6. členu ZVOP-2 in le za namen, ki je določen z zakonom oziroma ga pred obdelavo določi upravljavec.
Obseg obdelave osebnih podatkov, vključno z namenom in pravno podlago za obdelavo osebnih podatkov, je zabeležen v evidenci dejavnosti obdelave osebnih podatkov, kot tudi v informacijah za posameznike. Slednje so objavljene na spletni strani upravljavca, za zaposlene pa so vključene v poglavje št. 5 tega pravilnika.
Osebne podatke lahko v imenu upravljavca obdelujejo le s strani zastopnika (predstojnik upravljavca) pooblaščene osebe.
V kolikor pooblastila niso posebej opredeljena v aktualnem aktu o sistemizaciji se šteje, da pooblaščena oseba pridobi pooblastila za obdelavo s sklenitvijo pogodbe o zaposlitvi za posamezno delovno mesto oz. vlogo za katero je upravljavec **določil pooblaščene osebe v Evidenci dejavnost obdelav** ali **vodi t.i. shemo pooblastil**, ki je sestavni del **Kataloga pooblastil** – **Katalog pooblastil.**

7. člen

(Trajanje obdelave osebnih podatkov)

Trajanje obdelave posameznih vrst osebnih podatkov je natančneje opredeljeno v 9. členu tega Pravilnika, zabeleženo je tudi v posamezni evidenci dejavnosti obdelave osebnih podatkov.

8. člen

(Posredovanje osebnih podatkov)

Za vsako posredovanje osebnih podatkov mora vlagatelj (pravna ali fizična oseba), ki je do podatkov upravičen, predložiti pisno vlogo (lahko kot elektronsko sporočilo) v vsebini, kot jo določa 41. člen ZVOP-2. Pisna vloga mora vsebovati:
1. podatke o vlagatelju zahteve (za fizično osebo: osebno ime, naslov stalnega ali začasnega prebivališča; za samostojnega podjetnika posameznika, posameznika, ki samostojno opravlja dejavnost, ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis vlagatelja oziroma pooblaščene osebe;
2. pravno podlago za pridobitev zahtevanih osebnih podatkov;
3. namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za dosego namena pridobitve;
4. predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni, ter navedbo organa ali drugega subjekta, ki obravnava zadevo;

5. vrste osebnih podatkov, ki naj se mu posredujejo;
6. obliko in način pridobitve zahtevanih osebnih podatkov.

Pred posredovanjem osebnih podatkov, se je upravljavec dolžan prepričati, da bo osebne podatke posredoval upravičeni osebi. V ta namen preveri identiteto vlagatelja zahteve, lahko tudi z vpogledom v uradni osebni dokument. Če je prosilec upravljavcu osebno znan, se o tem napravi uradni zaznamek.

Osebni podatki se vlagatelju zahteve posredujejo na naslov bivališča, ki ga je navedel v zahtevi, ali na elektronski naslov, s katerega je posredoval zahtevo.

Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, določenimi s tem pravilnikom, ki preprečujejo razkritje osebnih podatkov nepooblaščenim osebam.

Osebni podatki se pošiljajo naslovnikom v zaprtih kuvertah, preko varnih informacijskih povezav (HTTPS, SSL, SSH) ali s posredovanjem prilog po elektronski pošti, ki so zaščitene z gesli. Če je to mogoče, se gesla za odpiranje prilog v elektronski pošti pošljejo po drugem komunikacijskem kanalu, kot elektronska pošta.

Posebne vrste osebnih podatkov se lahko upravičenim osebam posredujejo preko elektronskih komunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom. Praviloma je posredovanje posebnih vrst osebnih podatkov po elektronski poti tudi elektronsko podpisano z naprednim elektronskim podpisom. Posebne vrste osebnih podatkov se v papirni obliki pošiljajo po priporočeni pošti. Predlaga se, da se pošiljajo priporočeno s povratnico. Vsa prejeta dokazila o priporočenem posredovanju, prejete povratnice in drugi dokazi o tovrstnem pošiljanju se hrani skladno z roki hrambe, določenimi v veljavnem Enotnem klasifikacijskem načrtu (EKN) ali Obveznem okviru klasifikacijskih znakov, v kolikor EKN ne obstaja.

Upravljavec ne sme posredovati originalnih dokumentov, razen v primeru pisne odredbe sodišča oziroma, če tako zahtevajo veljavni predpisi, sicer vselej pošlje le kopijo, ki jo na željo vlagatelja zahteve lahko označi s pripisom, da je enaka originalu.

Upravljavec vodi in hrani evidenco o posredovanju osebnih podatki v papirni ali digitalni obliki. Evidenca vsebuje informacije o tem: kateri osebni podatki so bili posredovani, komu, kdaj in na kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka.

Informacije iz prejšnjega odstavka upravljavec hrani dve leti, razen če drug zakon za posredovanje posameznih vrst podatkov določa drugačen rok.

Obveznost beleženja v evidenci posredovanj osebnih podatkov ne velja, kadar je upravljavec osebne podatke zakonito objavil na svojih spletnih straneh ali na drug ustrezen način, in kadar gre za osebne podatke, za katere zakon določa, da so javni ali javno dostopni oziroma je obdelava dogovorjena s pogodbo.

9. člen

(Čas hrambe in brisanje osebnih podatkov)

Osebni podatki se obdelujejo, dokler ni dosežen namen obdelave, potem se anonimizirajo ali izbrišejo. Če je rok hrambe določen z zakonom, se osebni podatki hranijo v tem času, sicer pa v odvisnosti od pravnega temelja za obdelavo.
Izjemoma se lahko obdobje hrambe osebnih podatkov podaljša v primerih kot so:

- tekoči postopki pristojnih organov Republike Slovenije ali organov drugih držav članic EU, če obstaja verjetnost, da bo upravljavec potreboval zapise osebnih podatkov, da dokaže skladnost svojega ravnanja z veljavnimi predpisi ali
- tekoče pravdne ali druge podobne (na primer arbitražne, mediacijske, konciliacijske) zadeve, pri katerih obstaja verjetnost, da bo upravljavec potreboval zapise osebnih podatkov.

Brisanje osebnih podatkov v informacijskih sistemih, ki predstavljajo metapodatke ali elemente za priklic gradiva iz dolgoročne e-hrambe, se ne izvaja pred izbrisom gradiva, ki je povezano s temi metapodatki. Vse aktivnosti z dokumentarnim in arhivskim gradivom v eHrambi Logitus upravljavec izvede skladno z določbami prevzetih vzorčnih notranjih pravil Logitus.
Dokumentarno gradivo in z njim povezane osebne podatke je upravljavec dolžan hraniti najmanj do najkrajšega roka hrambe, ki je opredeljen v veljavnem enotnem klasifikacijskem načrtu (EKN) za VIZ. Arhivsko vzorčno in arhivsko gradivo ter z njim povezane podatke (tudi osebne podatke) pa je upravljavec dolžan hraniti do dokumentirane izvedbe postopkov odbiranja, izločanja ter izročanja gradiva pristojnim arhivom skladno z njihove strani prejetimi navodili za odbiranje in strokovno tehničnimi navodili.

4. UKREPI ZA VARNO OBDELAVO OSEBNIH PODATKOV

10. člen

(Obveznost in odgovornost za izvajanje ukrepov)

Izvajanje organizacijskih ukrepov za varnost osebnih podatkov so dolžni zagotoviti vsi zavezanci po tem pravilniku (zaposleni in drugi pogodbeni sodelavci, ki prihajajo v stik z osebnimi podatki) skladno z delovnim mestom oz. vlogo na katerem so zaposleni.
Ukrepi za zakonito in varno obdelavo osebnih podatkov, ki jih je dolžan izvajati obdelovalec, se določijo s pogodbo z obdelovalcem.

11. člen

(Obvezni ukrepi za varno obdelavo OP)

Upravljavec za preprečevanje nepooblaščenega dostopa, razkritja ali posredovanja osebnih podatkov ali druge obliko zlorabe osebnih podatkov izvaja naslednje ukrepe:

- Organizacijski ukrepi:
  - dosledno vodenje evidenc dejavnosti obdelave osebnih podatkov ter oznaka posebnih vrst osebnih podatkov na evidenci, ki takšne podatke vsebuje;

- dosledno vodenje seznama (internih in zunanjih) pooblaščenih oseb za obdelavo osebnih podatkov, izjav o varstvu osebnih podatkov in informiranje ter usposabljanje pooblaščenih oseb za obdelavo osebnih podatkov (t.i. sheme pooblastil);
- sklepanje pogodb o obdelavi osebnih podatkov z zunanjimi pogodbenimi obdelovalci osebnih podatkov, ter po potrebi vnos določb o pomenu varstva osebnih podatkov v pogodbe o zaposlitvi in druge pogodbe z delavci, ki so pod neposrednim vodstvom upravljavca;
- ozaveščanje vseh (zaposlenih in drugih pogodbenih sodelavcev) oseb, ki so jim dodeljena pooblastila za obdelavo osebnih podatkov, o relevantnih določilih tega pravilnika, ter o njihovih obveznostih in odgovornostih v zvezi z varstvom osebnih podatkov;
- izvajanje rednih obdobnih (predvidoma letnih, lahko pa tudi pogostejših) pregledov nad ravnanjem oz. obdelavo osebnih podatkov (notranje kontrole).

- Tehnični ukrepi:
  - zagotavljanje lastnih uporabniškim imen in drugih osebnih poverilnic za prijavo v informacijske sisteme, kjer se vrši obdelava osebnih podatkov;
  - zagotavljanje nadgradnje sistemske in antivirusne programske opreme na vseh računalnikih in strežnikih pri upravljavcu, kjer se izvaja obdelava osebnih podatkov;
  - uveljavljanje načela brezpogojne periodične menjave gesel v VIZ informacijskih sistemih;
  - preprečevanje možnosti skupinske prijave v VIZ informacijske sisteme;
  - uporaba osebnih kvalificiranih digitalnih potrdil za elektronsko podpisovanje ter dostopa do eHrambe Logitus;
  - sprotno ažuriranje pooblastil odgovornih oseb v informacijskih sistemih skladno z dejanskim stanjem in organizacijskimi spremembami;
  - uporaba zgolj elektronske pošte, ki jo dodeli upravljavec;
  - zagotavljanje varnosti pri dostopu do spleta.

4. 1 Evidence dejavnosti obdelav osebnih podatkov

12. člen

(Evidenca dejavnosti obdelav osebnih podatkov)

Upravljavec vodi Evidenco dejavnosti obdelav osebnih podatkov, ki vsebuje vse dejavnosti obdelav osebnih podatkov upravljavca (v nadaljnjem besedilu: evidence OP).
Vsaka evidenca OP vsebuje vse naslednje informacije:

- o upravljavcu in pooblaščeni osebi za varstvo podatkov (DPO);
- namen obdelave;
- opis kategorij posameznikov, na katere se nanašajo osebni podatki,
- vrste osebnih podatkov in, kadar je to primerno, oznako, da gre za posebno vrsto osebnih podatkov;
- uporabnike ali kategorije uporabnikov, ki so jim ali jim bodo lahko razkriti osebni podatki;

- informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo;
- roke hrambe oziroma izbrisa različnih vrst podatkov;
- splošen opis varovanja osebnih podatkov in
- pravno podlago za obdelavo osebnih podatkov.

Upravljavec vodi in hrani evidence OP v dokumentarnem sistemu v papirni ali elektronski obliki.

4. 2 Pooblaščene osebe za obdelavo osebnih podatkov

13. člen

(Pooblaščene osebe za obdelavo osebnih podatkov)

Pooblaščene osebe za obdelavo osebnih podatkov so odgovorne za zakonito obdelavo ter varstvo in varnost osebnih podatkov iz posameznih evidenc OP. Obveza varovanja osebnih podatkov, s katerimi se pooblaščena oseba seznani pri svojem delu, traja tudi po prenehanju delovnega razmerja pri upravljavcu oziroma dela zanj, in sicer časovno neomejeno.
Pooblaščene osebe oz. vloge ali istovrstna delovna mesta se vpiše v **Katalog pooblastil** v odvisnosti od presoje upravljavca pri čemer se pri poimenskem vpisu pooblaščenih oseb praviloma navede:

- naziv delovnega mesta (v primeru podelitve skupinskih pooblastil po vlogah) ali ime in priimek posamezne pooblaščene osebe za obdelavo osebnih podatkov;
- datum podelitve, spremembe in ukinitve pooblastila (v kolikor le-ta ni razvidna iz revizijske sledi posameznega informacijskega sistema oz. ni sklenjena pogodba o zaposlitvi oz. pogodba o poslovnem sodelovanju iz katere je mogoče razbrati pričetek in zaključek pooblastila povezanega z razporeditvijo na delovno mesto ali opravljanjem dogovorjenih del);
- navedba vrst OP (npr. dokumentacija o vzgojno izobraževalnem procesu), za katere so pooblaščeni zaposleni;
- raven dostopa do osebnih podatkov znotraj posameznega informacijskega sistema, kadar je to relevantno (opcijsko).

V primeru vnosov vlog oz. istovrstnih delovnih mest upravljavec na poljuben način vodi evidenco oseb, ki so zaposlene na določenem istovrstnem delovnem mestu. V primeru vlog oz. istovrstnih delovnih mest se v Katalog pooblastil posameznih pooblaščenih oseb ne vnaša.
Vse pooblaščene osebe, ki dostopajo do osebnih podatkov pri upravljavcu podpišejo izjavo o varstvu osebnih podatkov - **Izjave za zaposlene in zunanje**.

14. člen

(Dostop do informacijskih rešitev)

Pooblaščena oseba za obdelavo osebnih podatkov, ki pri svojem delu potrebuje dostop do informacijskih rešitev, se loči (vsaj) na:

- testnega uporabnika – uporabnik z dostopom do testnega okolja;
- uporabnika – običajen uporabnik;
- administratorja – administrator v posamezni rešitvi.

Pooblaščena oseba za obdelavo osebnih podatkov mora z ustreznimi ukrepi skrbno varovati zaupnost ter ne sme nikoli posredovati ali razkriti svojega uporabniškega imena in gesla, certifikata (digitalno potrdilo) ali podatkov o dvofaktorski avtentikaciji za katerikoli dostop drugi osebi, niti ne nadrejeni osebi ali sodelavcu/-ki.
Tehnološka sredstva za prijavo v posamezen informacijski sistem morajo omogočati prijave iz katerih je mogoče nesporno ugotoviti, kdo je posamezen informacijski sistem uporabil, tudi zgolj vstopil vanj.

4. 3 Pooblaščena oseba za varstvo podatkov (DPO)

15. člen

(Imenovanje DPO)

Upravljavec določi in imenuje pooblaščeno osebo za varstvo podatkov skladno z določbami ZVOP-2. O imenovanju pooblaščene osebe za varstvo podatkov se obvestijo tudi zaposleni, ki se lahko za posvetovanje obračajo neposredno nanjo.

4. 4 Pogodbena obdelava osebnih podatkov

16. člen

(Obdelovalci)

Posamezna opravila v zvezi z obdelavo osebnih podatkov v imenu upravljavca lahko opravlja obdelovalec osebnih podatkov (obdelovalec), ki je registriran za opravljanje takšne dejavnosti in zagotavlja postopke in ukrepe za varnost in varstvo osebnih podatkov, ki so potrebni za varstvo podatkov pred naključnim ali nezakonitim uničenjem ali naključno izgubo, spreminjanjem, nepooblaščenim posredovanjem ali dostopom ali katerim koli drugim nezakonitim načinom obdelave.
Pogodbeno obdelavo osebnih podatkov pri obdelovalcu ureja pogodba. Pogodba o obdelavi osebnih podatkov mora biti skladna z 28. členom Splošne uredbe o varstvu podatkov.
Pogodba mora biti pisna v fizični (papirni) ali elektronski obliki.
Upravljavec sklepa dogovore z obdelovalci, ki zagotavljajo primerljiv način ukrepov za varnost osebnih podatkov, kakor ga predvideva ta pravilnik.
Upravljavec vodi evidenco sklenjenih pogodb z obdelovalci.

4. 5 Interne presoje skladnosti dejavnosti obdelav osebnih podatkov z veljavnimi predpisi

17. člen

(Presoje skladnosti)

Upravljavec mora redno izvajati interne presoje skladnosti izvajanja dejavnosti obdelave osebnih podatkov z veljavnimi predpisi. Presoje skladnosti se izvajajo praviloma enkrat letno.

4. 6 Predhodna izvedba DPIA

18. člen

(Ocena učinka v zvezi z varstvom osebnih podatkov)

Upravljavec je dolžan izvesti oceno učinka v primerih iz 35. člena Splošne uredbe o varstvu podatkov.
Ocena učinka v zvezi z varstvom podatkov iz 1. odstavka se zahteva zlasti v primeru:

a) sistematičnega in obsežnega vrednotenja osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, vključno z oblikovanjem profilov, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo;
b) obsežne obdelave posebnih vrst podatkov ali
c) obsežnega sistematičnega spremljanja javno dostopnega območja.

5. POLITIKA VARSTVA OSEBNIH PODATKOV ZAPOSLENIH

19. člen

Elektronska pošta, računalnik (prenosni in stacionarni), mobilni telefon in druge elektronske naprave, ki jih delavcu za potrebe opravljanja dela dodeli delodajalec, se s strani zaposlenih uporabljajo v službene namene.
Vsakemu delavcu, ki pri delu uporablja računalnik, se dodeli službeni e-naslov, ki ga je dolžan uporabljati v zvezi z delom tako za komunikacijo znotraj delodajalca kot za komunikacijo v imenu delodajalca navzven.
Elektronsko poslovanje s strankami (ministrstvo, starši in tretjimi) pri upravljavcu praviloma poteka preko elektronskega naslova tajnistvo@os-vrhovci.si, do katerega ima dostop poslovni sekretar oz. tajnik VIZ. Delavec je dolžan e-sporočilo, ki je pomembno za upravljavca, prejel pa ga je na osebni službeni elektronski naslov, najkasneje v 24-urah od prejema posredovati na omenjeni e-naslov upravljavca.
Elektronski naslov delavca, ki je angažiran bodisi na podlagi pogodbe o zaposlitvi bodisi na drugem pogodbenem temelju, se ukine z dnem prenehanja delovnega ali drugega pogodbenega razmerja.

V omejenem obsegu in razumnih mejah se lahko službena elektronska pošta, službeni računalnik in službeni telefon uporabljajo tudi v zasebne namene delavcev, pri čemer so se delavci na strani upravljavca dolžni v smislu skrbi za ugled VIZ ustanove izogibati pošiljanju in prejemanju elektronskih sporočil z neprimerno in žaljivo vsebino in drugi rabi službene opreme, ki lahko negativno vpliva na položaj in interese delodajalca – upravljavca.

20. člen

V računalnik (delovno postajo), drugo tehnično sredstvo (na primer mobilni telefon, tablico), dano v uporabo s strani upravljavca, ali v elektronsko pošto delavca, ki je angažiran bodisi na podlagi pogodbe o zaposlitvi bodisi na drugem pogodbenem temelju (v nadaljevanju: uporabnik opreme), sme upravljavec poseči le v izjemnih primerih, opredeljenih v tem pravilniku, in sicer v primeru nepričakovane, nenadne in dalj časa trajajoče ali trajne odsotnosti uporabnika opreme, na primer v primeru odpovedi delovnega razmerja s strani zaposlenega brez odpovednega roka, v primeru odpovedi delovnega razmerja iz krivdnih razlogov zaradi neopravičene odsotnosti, v primeru, da zaradi svojega zdravstvenega stanja uporabnik opreme ni sposoben izraziti svoje volje, pa takšno stanje traja dlje časa ali se upravičeno domneva, da bo trajalo dlje časa, smrt uporabnika opreme in podobni izredni primeri, kadar:
- je to nujno potrebno za izpolnitev zakonskih obveznosti upravljavca;
- je to nujno in neogibno potrebno za izpolnitev pogodbenih obveznosti upravljavca, katerih neizpolnitev ali izpolnitev z zamudo bi za upravljavca lahko pomenila izgubo ugleda ali nastanek premoženjske škode.

Uporabnika opreme se pred posegom v njegov računalnik (delovno postajo), drugo tehnično sredstvo ali elektronsko pošto pozove k prostovoljni predložitvi gesel in/ali potrebnih dokumentov ter se mu za izpolnitev zahteve postavi primeren rok, ki ni krajši od 8 ur. Tako v primeru prostovoljnega posredovanja dostopnih gesel, kot tudi v primeru, da se uporabnik opreme na poziv upravljavca ne odzove ali ga zavrne, se vstop v računalnik (delovno postajo), drugo tehnično sredstvo ali elektronsko pošto opravi s strani osebe, ki jo vsakokrat imenuje zastopnik oz. predstojnik upravljavca, delavcu/uporabniku opreme pa se omogoči, da dejanju osebno prisostvuje, tako da se ga obvesti o kraju in času dejanja, razen če to iz objektivnih razlogov ni mogoče ali če zaposleni s svojim ravnanjem očitno onemogoča vstop.

O vsakem vstopu v računalnik, drugo tehnično sredstvo in/ali elektronsko pošto po tem členu se vodi dokumentacija, ki vsebuje najmanj:

- obrazložen razlog za dopustnost vstopa (vključno z analizo zakonitega interesa kot pravnega temelja, s katero se je upravljavec prepričal, da v konkretnem primeru njegov zakoniti interes pretehta nad pravicami in svoboščinami delavca);
- zapisnik o vstopu v računalnik ali elektronsko pošto z morebitnimi pripombami delavca, če je ta navzoč;
- navedbo prisotnih oseb;
- seznam oziroma izpis pridobljenih podatkov.

Šteje se, da je o namenu uporabe elektronske pošte in ostale programske opreme, ki jo uporabniku opreme za namene opravljanja dela nudi upravljavec, ter o možnostih nadzora po določbah tega člena tega pravilnika uporabnik opreme predhodno obveščen, ko se seznani s tem pravilnikom.

21. člen

Vpogled v telefonske prometne podatke mobilnih naročniških številk v lasti upravljavca in uporabi posameznega uporabnika opreme, lahko od operaterjev telekomunikacijskih storitev zahteva le zastopnik oz. predstojnik upravljavca ali od njega pooblaščena oseba in le v primeru spora med uporabnikom opreme in upravljavcem o višini stroškov porabe za sporno mobilno naročniško številko za določeno obračunsko obdobje, pri čemer to stori skladno z določili zakona, ki ureja elektronske komunikacije, in nikakor ne sme preverjati identitete oziroma lastništva klicanih ali kličočih številk, razen kadar bi to zaradi ugotavljanja, ali so bili klici opravljeni v službene namene, zahteval delavec/uporabnik opreme sam.
Upravljavec mobilnim napravam v njegovi lasti in v uporabi posameznega uporabnika opreme ne sme slediti in v ta namen v svoje mobilne naprave ne sme namestiti naprave oziroma aplikacije za sledenje uporabniku opreme.
Šteje se, da je o namenu uporabe službenih mobilnih telefonov, ki jo uporabniku opreme za namene opravljanja dela nudi upravljavec, o kriterijih za dodelitev, vodenju evidenc in prenehanju upravičenja uporabnik opreme obveščen, ko mu upravljavec izroči izvod tega Pravilnika.

22. člen

Delavec lahko za namene opravljanja dela poleg službene opreme in naprav v lasti upravljavec uporablja svoj zasebni računalnik in/ali mobilni telefon in druge tehnične naprave, če takšno uporabo odobri zastopnik oz. predstojnik ali od njega pooblaščena oseba, ki preveri uporabo z vidika varnosti za obdelavo osebnih podatkov upravljavca.
V primeru prenehanja delovnega razmerja je delavec dolžan iz zasebnih računalnikov in/ali mobilnih telefonov ali drugih naprav (tudi USB ključev ipd.), ki jih je v soglasju z delodajalcem uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni s službenega omrežja, in vse datoteke, ki jih je zaposleni uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.
Ob prenehanju delovnega razmerja delodajalec delavcu v podpis praviloma ponudi izjavo, da je s službenega računalnika, drugih tehničnih naprav in iz predala elektronske pošte izbrisal vsebine, ki so bile zasebne narave (kot na primer fotografije), in je naprava primerna za čiščenje podatkov z nje« oziroma za predajo v uporabo drugemu uporabniku opreme.
Delavec s podpisom izjave potrdi, da z vidika varstva osebnih podatkov in varstva zasebnosti širše ni zadržkov glede dostopanja delodajalca ali z njegove strani pooblaščenega pogodbenega sodelavca do delovnih sredstev, vključno s predalom e-pošte, ki jih je do tedaj uporabljal sam. Kolikor ima zadržke, se delavcu omogoči, da ob prisotnosti pooblaščenega delavca z delovnih sredstev prenese zasebne vsebine na zunanji nosilec in jih na delovnem sredstvu izbriše.

6. TEHNIČNI UKREPI ZA VARNO OBDELAVO OSEBNIH PODATKOV

23. člen

(Prostori in nosilci osebnih podatkov)

Nosilci osebnih podatkov so vsak računalniški ali elektronski nosilec podatkov, vsak dokument (v papirni ali elektronski obliki), na katerem je zapisan osebni podatek in strojna ter programska oprema. Varovani morajo biti z organizacijskimi ukrepi, določenimi s tem pravilnikom, ki nepooblaščenim osebam onemogočajo dostop do osebnih podatkov.

Nepooblaščene osebe ne smejo vstopati v prostore, kjer se nahajajo osebni podatki brez spremstva ali prisotnosti pooblaščenega zaposlenega delavca. Delavec, ki dela v teh prostorih, mora vestno in skrbno nadzorovati prostor, vstope in izstope iz prostora ter ob zapustitvi prostor zakleniti. V kolikor so pri upravljavcu nameščena druga tehnična sredstva za preprečevanje oziroma odkrivanje nepooblaščenih vstopov v prostore (na primer alarmni sistem, video nadzorni sistem, v kolikor upravljavec z njim razpolaga), je treba ta sredstva dosledno uporabljati.

Delavec, ki pri delu obdeluje osebne podatke, nosilcev osebnih podatkov ne sme puščati nenadzorovanih ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam oziroma nepooblaščenim delavcem.

V prostorih, v katere imajo vstop uporabniki storitev oziroma osebe, ki niso zaposlene pri upravljavcu oziroma niso pooblaščene za obdelavo osebnih podatkov, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da je uporabnikom storitev in drugim nepooblaščenim osebam onemogočen vpogled oz. dostop do osebnih podatkov. Nastavljeni morajo biti tudi ohranjevalniki zaslona za čas neaktivnosti delavca na računalniški opremi.

Poslovni partnerji in drugi obiskovalci se smejo gibati v prostorih upravljavca le ob prisotnosti delavca, ki mora skrbeti za to, da je dostop ali vpogled v nosilce podatkov nepooblaščenim osebam onemogočen. Prostori upravljavca se morajo redno zaklepati, s čimer se nepooblaščenim osebam prepreči nenapovedan oziroma nedovoljen vstop.

Tehnično-vzdrževalni delavci in čistilke se lahko gibljejo v poslovnih prostorih izven delovnega časa in brez prisotnosti pooblaščenega delavca le, če so nosilci osebnih podatkov shranjeni v zaklenjenih omarah ali arhivu (npr. ognjevarni sef oziroma omare), tehnično-vzdrževalni delavci in čistilke pa nimajo ključev teh omar ali arhivov oziroma so osebni podatki shranjeni na za njih nedostopnih elektronskih medijih.

Delavci, ki zaznajo nepooblaščen vstop v prostore upravljavca, nepooblaščen dostop do omar, medijev, programov ali opreme, na kateri se nahajajo osebni podatki, ali sum takega ravnanja, morajo o tem nemudoma obvestiti zastopnika oz. predstojnika ustanove. Slednji, po potrebi s posvetovanjem s pooblaščeno osebo za varstvo podatkov, presodi (predvsem upoštevajoč namen nepooblaščenega vstopa ali dostopa), kakšna so potrebna nadaljnja ravnanja (na primer ozaveščanje delavcev, izboljšanje sistema varovanja, disciplinski postopki, obvestitev pristojnih organov) ter po potrebi poda priporočilo zakonitemu zastopniku upravljavca.

24. člen

(Vstop zaposlenih v pisarne)

Za dostop do pisarne je potrebno imeti ključe pisarne in vstopno alarmno kodo. Ključe/kartice in dostopne kode dodeli zastopnik upravljavca. Dvojnike ključev pisarne je delavcem prepovedano izdelovati, razen v kolikor to ni izrecno naročeno delavcu s strani direktorja/ravnatelja.

Ključev se ne sme puščati v ključavnici v vratih z zunanje ali notranje strani. Ključa/dostopne kartice ali vstopne alarmne kode delavec ne sme posojati, dajati ali razkrivati drugim osebam, niti v kolikor so to drugi delavci. V primeru izgube ali kraje mora delavec nemudoma obvestiti zastopnika upravljavca oziroma drugo osebo, ki ji je pri upravljavcu dodeljeno skrbništvo nad ključi, dostopnimi karticami oziroma alarmnimi kodami.

25. člen

(Ukrepi za varovanje sistemske in aplikativne računalniške opreme)

Dostop do računalniške programske opreme, kjer so shranjeni osebni podatki, mora biti varovan na način, ki omogoča dostop samo pooblaščenim delavcem.
Računalniki, na katerih se obdelujejo osebni podatki, morajo biti ustrezno zaščiteni s sodobno antivirusno zaščito, imeti nameščen ohranjevalnik zaslona in nastavljeno omogočanje avtomatičnih popravkov operacijskega sistema.
Delavci oziroma pooblaščene osebe za obdelavo osebnih podatkov morajo upoštevati vsa interna navodila v zvezi z računalniško opremo in temu primerno računalnike tudi uporabljati.
Upravljavec zagotavlja, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja strojne, sistemske ali aplikativne programske opreme z osebnimi podatki ob morebitnem kopiranju, po prenehanju potrebe po kopiji, kopija brez nepotrebnega odlašanja uniči.
Pooblaščena oseba upravljavca mora biti v času servisiranja računalnika ali programske opreme, ki vsebuje osebne podatke, ves čas prisotna in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki, zlasti v primeru, če se v računalniku nahajajo osebni podatki posebne vrste.
Dostop do osebnih podatkov mora biti vedno zavarovan vsaj z geslom za prijavo v računalnik.
Namenska, osebna gesla se redno spreminjajo, zlasti pa ob vsakem sumu, da je prišlo do zlorabe gesla. Novo geslo ne sme biti enako ali podobno prejšnjemu, vsaj za 3 predhodna gesla. Minimalna dolžina se prilagaja priporočilom Informacijskega pooblaščenca oz. tehničnim zmožnostim posamezne informacijske rešitve in praviloma vsaj 8 alfa numeričnih znakov za prijavo v informacijske sisteme za obdelavo podatkov s področja VIZ.

Gesel za dostop do osebnih podatkov se ne sme shranjevati na papirju ali na način, da je dostop do gesel omogočen nepooblaščenim osebam. V primeru zlorabe gesla ali suma zlorabe gesla, je potrebno geslo nemudoma spremeniti ter o zlorabi gesla ali sumu zlorabe gesla obvestiti internega koordinatorja za varstvo podatkov, osebo, ki je odgovorna za dodeljevanje gesel, ali zakonitega zastopnika upravljavca.
Delavec, ki ima dostop do katerekoli informacijske rešitve ali evidence, mora pri delu z osebnimi in zaupnimi podatki ravnati še posebej skrbno, da se ne razkrijejo osebni podatki nepooblaščeni osebi ali razkrijejo zaupni podatki, ki se štejejo za poslovno skrivnost upravljavca ali njegovih pogodbenih partnerjev.
Delavec ne sme nikoli posredovati ali razkriti svojega uporabniškega imena, gesla ali certifikata (digitalno potrdilo) za katerikoli dostop nepooblaščeni osebi, temveč mora zaupnost teh podatkov varovati z najvišjo skrbnostjo.
Razkritje uporabniškega imena, gesla ali certifikata drugi osebi pomeni kršitev varstva osebnih podatkov, ter kršitev obveznosti iz pogodbe o zaposlitvi. Lahko predstavlja tudi razlog za odškodninske zahteve, pa tudi naznanitev pristojnim organom za kazenski pregon.

7. VIDEONADZOR

26. člen

Videonadzor je namenjen varnosti ljudi ali premoženja in zagotavljanju nadzora vstopa v te prostore ali izstopa iz njih. Odločitev o videonadzoru je sprejel zastopnik upravljavca, sledeč načelu minimalnega obsega osebnih podatkov, ki se obdelujejo.
Obvestilo o izvajanju video-nadzora je nameščeno pred vstopom v področje videonadzora. Posamezniku je na ta način omogočeno, da se seznani z izvajanjem videonadzora in da se lahko vstopu v nadzorovano območje odpove.
Obvestilo o izvajanju videonadzora mora poleg informacij iz 13. člena Splošne uredbe vsebovati naslednje informacije:
1. pisno ali nedvoumno grafično opisano dejstvo, da se izvaja videonadzor;
2. namene obdelave, navedbo upravljavca videonadzornega sistema, telefonsko številko ali naslov elektronske pošte ali spletni naslov za potrebe uveljavljanja pravic posameznika s področja varstva osebnih podatkov;
3. informacije o posebnih vplivih obdelave, zlasti nadaljnje obdelave;
4. kontaktne podatke pooblaščene osebe (telefonska številka ali naslov e-pošte);
5. neobičajne nadaljnje obdelave, kot so prenosi subjektom v tretje države, spremljanje dogajanja v živo, možnost zvočne intervencije v primeru spremljanja dogajanja v živo.
Namesto objave v obvestilu iz prejšnjega odstavka se lahko obveščanje o videonadzoru izvaja na način, da se informacije iz 13. člena Splošne uredbe in informacije iz 3. do 5. točke prejšnjega odstavka objavijo na spletnih straneh upravljavca. Na obvestilu iz o izvajanju videonadzora dostopa v poslovne prostore pa je objavljen spletni naslov, kjer so dostopne vse informacije.

Video-nadzorni sistem, s katerim se izvaja videonadzor, je zavarovan pred dostopom nepooblaščenih oseb. V kolikor se izvaja videonadzor s pomočjo računalniške opreme, ki je v rabi tudi za druge namene (npr. omrežni diski z možnostjo shranjevanja in upravljanja videonadzora) mora biti dostop do te opreme zaščiten s prijavnim imenom in geslom ter dvofaktorsko prijavo na drugem sredstvu (npr. telefon).

27. člen

Zbirka osebnih podatkov, ki nastaja samodejno na video-nadzornem sistemu, vsebuje posnetek posameznika: slika oziroma glas, če to kamera omogoča in beleži tudi datum in čas, ki je povezan z vstopom, premikanjem ali izstopom iz poslovnega prostora oz. področja v njem, kjer se videonadzor izvaja.
Posnetki se hranijo največ 90 dni od nastanka, potem se samodejno nepovratno uničijo.
O izvajanju videonadzora in o vsebinah iz obvestila o izvajanju videonadzora so pisno obveščeni vsi zaposleni ter vsi drugi z obvestilom na mestu vstopa v poslovni prostor.
Vsi zaposleni se ob seznanitvi s tem pravilnikom še dodatno seznanijo z dejanskim obsegom izvajanjem videonadzora – vključno z informacijami iz 13. člena tega pravilnika.
V kolikor v ustanovi ne deluje reprezentativni sindikat, svet delavcev ali delavski zaupnik, posvetovanje po 78/VI členu ZVOP-2 ni potrebno izvesti.

28. člen

Video posnetki videonadzora pri upravljavcu se hranijo izključno na snemalni napravi. Dostop do posnetkov se avtomatizirano beleži v snemalni napravi (t.i. log datoteke, ki predstavljajo evidenco o videonadzoru) ter je omogočen samo pooblaščenim osebam za videonadzor. Vzroki za vpogled v video posnetke videonadzora so lahko: zahteva po zakonu upravičenega subjekta, odredba sodišča ali policije, varnostni incident (kot npr. vlom, kraja, alarmni dogodek, samodejno zaznano gibanje v službenih prostorih izven delovnega časa, ipd.) ter po nalogu zastopnika ustanove, kadar je podan sum, da je prizadeta z videonadzorom varovana dobrina.

Vsak dostop do posnetkov videonadzornega sistema se dokumentira s podatki:
- razlog za dostop;
- obseg dostopa;
- pooblaščena oseba, ki je dostop opravila (ime, priimek, delovno mesto, delodajalec);
- datum, kraj in čas dostopa;
- pooblaščena oseba, ki je posnetke prevzela (ime, priimek, delovno mesto, delodajalec), kraj in datum prevzema posnetkov;
- podatek o tem, kje se hranijo iz sistema eventualno izvzeti posnetki.

Evidenca dostopov ter evidenca posredovanja posnetkov tretjim osebam se hrani tri leta po opravljenem dostopu oz. posredovanju.

8. POLITIKA VARNOSTNIH INCIDENTOV

29. člen

(Kršitev varstva osebnih podatkov)

Za kršitev varstva osebnih podatkov šteje vsaka obdelava osebnih podatkov brez pravnega temelja (tudi v nasprotju z namenom, za katerega so bili osebni podatki pridobljeni).

Kot zloraba šteje tudi kršitev varnosti osebnih podatkov, to je kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

Za poskus kršitve šteje poskus obdelave osebnih podatkov v nedovoljene namene oziroma brez pravnega temelja. Zastopnik upravljavca mora zoper tistega, ki je kršil varstvo osebnih podatkov ustrezno ukrepati.

Za kršitev varstva osebnih podatkov se šteje, na primer:

- nepooblaščen vpogled v osebne podatke;
- nepooblaščeno odkrivanje oziroma razkrivanje osebnih podatkov;
- nepooblaščeno uničenje;
- nepooblaščeno spreminjanje;
- poškodovanje zbirke;
- vdor v zbirko osebnih podatkov;
- prilaščanje osebnih podatkov.

30. člen

(Ukrepanje ob ugotovitvi kršitve varstva osebnih podatkov)

Kdorkoli, ki izve ali opazi, da je prišlo do kršitve varstva osebnih podatkov, mora o tem nemudoma obvestiti zastopnika oz. predstojnika upravljavca ali pooblaščeno osebo za varstvo podatkov.

Vsi zaposleni oziroma drugi delavci in pogodbeni obdelovalci morajo slediti navodilom zastopnika oz. predstojnika upravljavca in pooblaščene osebe za varstvo podatkov z namenom, da se čimprej zaustavi nadaljnje kršenje varstva osebnih podatkov oziroma nastanek škodljivih posledic ter se zavarujejo dokazi.

Vdor ali kakršenkoli drug informacijski varnostni incident je upravljavec dolžan dokumentirati.

Priporočljivo je, da upravljavec po vsakem odkritem incidentu kršitve varstva osebnih podatkov izvede analizo stanja ter identificira okoliščine, ki so omogočile ali znatno doprinesle k incidentu kršitve varstva osebnih podatkov. V zvezi s temi okoliščinami se opredeli tveganje njihove ponovitve ter predvidi ukrepe za zmanjšanje tega tveganja.

Predvideni ukrepi morajo biti sorazmerni glede na verjetnost ponovitve incidenta, resnost njegovih posledic ter naravo osebnih podatkov (resneje je treba obravnavati incidente v zvezi s posebnimi vrstami osebnih podatkov), pri čemer se upošteva tudi razpoložljive vire upravljavca.

V zvezi s predvidenimi ukrepi se določi rok in odgovorno osebo za njihovo izvedbo, ob poteku tega roka pa se dokumentira dejansko stanje ter oceni uspešnost implementacije ukrepov. Po potrebi se predlaga tudi spremembo tega pravilnika.

V primeru kršitve varnosti osebnih podatkov je zakoniti zastopnik upravljavca dolžan brez nepotrebnega odlašanja najpozneje v 72 urah po seznanitvi s kršitvijo o kršitvi obvestiti Informacijskega pooblaščenca.

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, je upravljavec dolžan o tem obvestiti posameznike, čigar osebnih podatki so bili zajeti v varnostni incident. Obveznost obveščanja ni podana, če ni izkazana verjetnost, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov, na katere se kršitev nanaša.

9. URESNIČEVANJE PRAVIC POSAMEZNIKOV

31. člen

(Pravice posameznikov)

Upravljavec mora posameznikom zagotoviti vse pravice, ki jih ima slednji po veljavnih predpisih kar opredeli v **Informacijah za posameznike**, ki so javno objavljene.

Upravljavec v okviru reševanja zahtev iz naslova uresničevanja pravic posameznikov po Splošni uredbi o varstvu podatkov vzpostavi in vodi **evidenco postopkov uresničevanja pravic posameznikov**, v katero vpisuje najmanj:

- posameznika, ki je zahtevo podal (ime, priimek, naslov bivališča, elektronski naslov ali drug podatek za komunikacijo);
- vsebino zahteve ali opravilno številko, pod katero se zadeva rešuje ter status reševanja zadeve;
- vrsta odločitve;
- postopek s pravnimi sredstvi.

Posamezne zahteve iz naslova uresničevanja pravic posameznikov upravljavec hrani v papirni ali elektronski obliki.

10. ZAUPNI PODATKI IN POSLOVNA SKRIVNOST

32. člen

(Varstvo zaupnih podatkov oziroma poslovne skrivnosti)

Zaposleni in druge osebe, ki so pooblaščene za dostop do podatkov upravljavca, morajo pri izvrševanju svojih funkcij oziroma delovnih obveznosti varovati zaupnost podatkov, za katere je upravljavec pisno določil, da so zaupne narave ter podatkov, za katere je mogoče v danih okoliščinah razumno sklepati, da se jih ohrani kot skrivnost. Podatke, ki so zaupne narave oziroma predstavljajo poslovno skrivnost po določbah Zakona, ki ureja poslovno skrivnost upravljavca, morajo osebe, ki do njih dostopajo, varovati tako, da:

- jih ne razkrivajo, posredujejo ali omogočajo kakršno koli drugačno seznanitev z njimi nepooblaščenim osebam;
- uporabljajo zaupne informacije zgolj za dovoljene namene njihove uporabe ter v najmanjšem potrebnem obsegu za dosego teh namenov;
- zaupne informacije razmnožujejo le v najmanjšem obsegu, ki je potreben za izpolnitev dovoljenih namenov njihove uporabe, pri čemer morajo zagotoviti, da je zaupnost kopij varovana enako, kot zaupnost izvirnih zaupnih informacij;
- na zahtevo odgovorne osebe upravljavca nemudoma uničijo vse zaupne informacije, v vseh oblikah, na vseh nosilcih ter vključno z vsemi kopijami, za katere odgovorna oseba tako določi. Tudi po morebitnem uničenju zaupnih informacij mora oseba, ki se je z informacijami seznanila, še vedno varovati njihovo zaupnost, skladno s tem pravilnikom.

11. PREHODNE IN KONČNE DOLOČBE

33. člen

(Kršitve določb tega pravilnika)

Zavezanci so seznanjeni, da lahko ravnanje, ki ni skladno s tem pravilnikom, povzroči negativne posledice, kot so izguba zaupanja uporabnikov storitev ali dobaviteljev upravljavca, pravdne, inšpekcijske ali prekrškovne postopke, finančne izgube in poslabšanje ugleda upravljavca. Zoper osebe, ki ravnajo v neskladju s tem pravilnikom, se lahko sprožijo ustrezni pravni postopki (delovnopravni postopek redne odpovedi iz krivdnega razloga zaradi kršitve pogodbe o zaposlitvi, odškodninski postopek, predlog za kazenski pregon...).

34. člen

(Končne določbe)

Ta pravilnik začne veljati naslednji dan po podpisu zastopnika upravljavca.

Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o zbiranju in varstvu osebnih podatkov Osnovne šole Vrhovci z dne 29. 1. 2015.